Cryptographic Protocol Analysis and Verification

NSA

Technical Director: Ed Zieglar

Team 1

February 11, 2022

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Bi-weekly Report 1

Team Members:

Evan Dow - Ashley Mahoney - Nawal Smith - Daniel Stricklin - Andrew Webb - Jordan Wilson

Faculty:

Dr. Jeffrey Kulick

A. Overview of Project

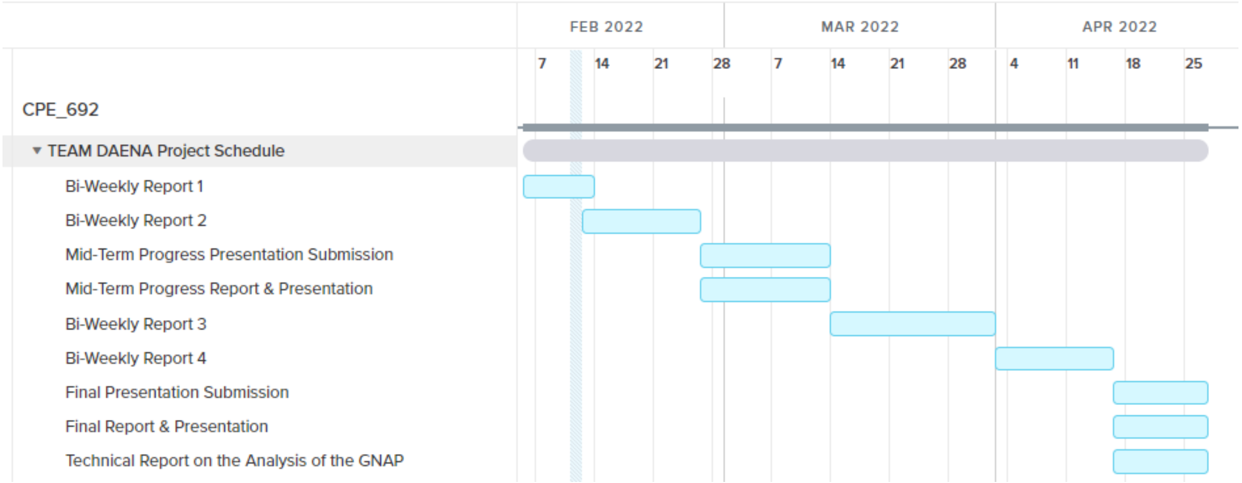
Our team acknowledges that there is no structure for the standardization of the cryptographic protocol, Grant Negotiation and Authorization Protocol (GNAP). Our goal is to focus on the analysis and verification of GNAP, a protocol that allows software to request delegated authorization to resource servers as well as request direct information. By utilizing the CPSA tool to conduct a formal analysis of this protocol we can use the generated shapes to infer weaknesses or security flaws that will provide a way to solidify the implementation.

B. Technical Approach

Understanding the cryptographic protocol, GNAP, through the verification analysis tool, CPSA through research, implementation and multiple in-depth training with our technical director.

C. Schedule

Attend bi-weekly meetings with our technical director to ensure we are on track. Attend weekly meetings within our group and with our professor.



D. Previous week’s work (February 1st - February 8th)

We met with our technical director on Wednesday, February 2nd, and Friday, February 4th, to learn more about the formal verification tool, CPSA, we will be using. Our technical director gave us an in-depth overview and training of the CPSA tool by providing numerous examples while we all reviewed the CPSA student guide. We also generated an initial draft of the GNAP Model, set up GNAP and CPSA training and recordings, and started working on preparing upcoming deliverables such as the bi-weekly report 1 and midterm progress report. Throughout this week we have made sure to update weekly the INSuRE dashboard and populate our trello cards with assigned tasks for every individual in the group.

E. This week's progress (February 8th - February 15th)

For this upcoming week's tasks we are reviewing GNAP RFC and starting to work on a draft for scheme input file, setting up the Git Repo for tracking our scheme file versions, setting up the CPSA tool on UAH servers, reviewing the CPSA training recordings to sharpen our understanding and ability of practicing with shapes, and completing the upcoming deliverable, bi-weekly report 1, all while making sure the weekly INSuRE dashboard is updated and the trello cards are populated with up-to-date assigned tasks for every individual in the group.

F. Issues

The main difficulty stems from the inexperience of group members with the CPSA tool as well as the GNAP being a fairly recent development when compared to existing cryptographic protocols. We will combat this by investing our initial resources heavily in research as well as training provided by our technical director. A question we have for our technical director is how do we model the data within the message within GNAP? I.e individual data types.